# SEL Table of Contents

# Section 5 - Cyber Security Enhancement Equipment

## Overview

This section lists equipment, software, and systems that contribute to improved information security. Four major functional categories are defined: encryption, host level security, network level security, and patch/configuration management. The items recommended in this section are included in the SEL because of the criticality of responders' information infrastructure in areas ranging from hazard assessment to communications and incident command. The increasing vulnerability of networks impacts the reliability of this infrastructure, and thus cyber security must be considered in deployment and response operations.

## Changes for 2006

This edition contains a considerably larger introduction, developed in conjunction with the DHS grant guidance used in the FY2006 Homeland Security Grant Program. The ICIS SubGroup contributed to the development of Appendix I in that guidance, and the discussion below was developed using that appendix as an initial draft. We have also updated the descriptions for all existing items in this section, and added new items entitled Forensic Software and Security Information Management Systems.

## Cyber Security Self-Assessment Questions and Resources

Agencies and jurisdictions at every level must have appropriate policies in place, understand their vulnerabilities, weigh the risks involved and make informed decisions on how to spend resources to secure systems and data. Some 10,000 new computer viruses were reported last year, and it now only takes a few minutes to compromise an unprotected computer that is connected to the Internet. A virus or other successful cyber attack can be devastating to networks, to the information contained within systems and, just as importantly, to the confidence of those who depend on these systems to accomplish their mission.

Information security is mission critical to every emergency responder. Every agency and jurisdiction should carefully consider three key components of information security:

- **confidentiality,** the ability to ensure that only authorized personnel/systems have access to any given data;
- **integrity,** the ability to ensure that data is not corrupted, and that only authorized personnel/systems can change any given data; and,
- **availability,** the ability to ensure that authorized personnel have timely and complete access to data whenever and wherever it is required.

The relative importance of these three components will vary among organizations. For example, fire dispatch may place a premium on availability at the expense of confidentiality, while an intelligence sharing center might sacrifice availability to ensure confidentiality. Ultimately, all three must be achieved to at least a minimal degree in order to meet mission requirements.

Each state and local government entity should develop and execute a comprehensive cyber security plan that demonstrates due diligence in cyber security. The goal of a cyber security plan is to identify the cyber threat environment, and address these threats in order to maintain confidentiality, integrity and availability sufficient for mission performance. The plan must account for factors such as limited staff and resources (and staff turnover); varying size and complexity of the organization; varying cyber security and technology knowledge base within the organization; and a wide variance in technology

being used. In addition to a developing a comprehensive plan, organizations must periodically test and exercise their plan, using vulnerability assessments to identify gaps in policy and technology, as well as training needs.

This plan must address four main functional areas: Policy, Training, Technology Deployment, and Vulnerability Assessment. Each of these areas supports the others, and together they meet emerging standards of due diligence in information security. The questions below are designed to assist in "self-assessment" and identify key issues within each major area. We have used the term "Organization" to represent a wide range of agencies, departments, and jurisdictions.

**Policy:**

- Does the Organization have a cyber security plan in place that sets the vision, goals, and objectives for Organization-wide cyber security?
- Has the Organization published a clear policy statement on cyber security to support the plan, including a "permitted use" policy for all Organization-owned cyber assets? Has this policy set been made available to subordinate organizations so that it can be adapted for their use?
- Does the Organization's policy statement provide a clear mechanism for feedback and use of vulnerability assessment results to refine policies, training, and technology deployment?
- Has the Organization established a certification/accreditation program for information systems?
- Does the Organization have a designated cyber security office/officer whose primary focus is on protecting the Organization's cyber infrastructure?
- Does the Organization have established cyber security metrics? Does the Organization have a mechanism for rating its cyber security alert level?
- Has the Organization established public, private, or academic partnerships for cyber security collaboration?
- Does the Organization have a capability for internal secure information sharing (Organization-wide secure portal)?
- Does the Organization have a formal connectivity policy covering network connections with external partners (including local government, state-wide intranet, etc.)? Does this policy address protection against intrusions via these connections?
- Does the Organization have a formal connectivity policy covering telecommuters or personnel who require access to internal systems from home or other off-site locations? If so, does this plan address vulnerabilities in offsite computers such as home computers that might be connected to the internal network?
- Does the Organization have a cyber operational center that functions 24/7? Does the Organization have an ad hoc 24/7 capability if an operational center does not exist?
- Does the Organization have an organization-wide Computer Security Incident Response Policy (IRP)? Is there a corresponding response plan, and are key personnel aware of their roles and all appropriate notification requirements?
- Does the Organization have a Continuity of Operations (COOP) plan that encompasses both communications and information technology capability?
- Does the Organization maintain a relationship with federal entities such as the United States Computer Emergency Readiness Team (US-CERT)?

**Training:**

- Does the Organization ensure that all employees have cyber security awareness training both at time of hire and on an annual recurring basis? Does this training include familiarization with

permitted use policies, and do employees sign an acknowledgement of their familiarity with the Organization's cyber security policies?

- Are training programs available at multiple levels commensurate with employees' responsibility (e.g., general awareness, system administrator, network administrator, etc.)?
- Does the Organization have an outreach program to ensure the greatest penetration possible for cyber security awareness throughout state and local governments?
- Does the Organization have a web presence that provides cyber security guidance?
- Does the Organization have a program to establish and maintain a set of best practices for cyber security, both for its own use and to share with local jurisdictions?

**Technology Deployment:**

- Is the technology deployed by the Organization justified in terms of identified cyber security threats and a valid risk management strategy?
- Has the Organization deployed appropriate technology for basic cyber security requirements such as anti-virus protection and firewalls on Internet-facing assets?
- Has the Organization deployed specific technology (including modifications and patches to existing systems and software) to respond to vulnerabilities identified by internal or third-party vulnerability assessments?
- Does the Organization have an asset management system that tracks the number, type, and location of their information technology assets? Does the Organization maintain a map of its network that depicts the position of these assets on its network? Does the system track personnel who are authorized access to cyber assets?
- Does the Organization have a system in place for tracking software versions in use, relevant known vulnerabilities, and available patches to counter those vulnerabilities?
- Does the Organization have cyber forensics capabilities to serve both civilian and criminal matters for the Organization?
- Does the cyber security technology deployed by the Organization have sufficient capability and capacity to function in both routine and crisis management conditions?
- Has the Organization addressed the physical security requirements of its cyber assets (e.g., physically isolating servers and network equipment, access control for server area, etc.)?

**Vulnerability Assessment:**

- Does the Organization have a formal program for periodic internal vulnerability assessment, and maintain a baseline of cyber threats and vulnerabilities?
- Does the Organization supplement its internal assessment program with third-party vulnerability assessments?
- Is there a formal risk management process by which assessment results are converted into prioritized remedial actions and tracked to completion?

While many of these questions are oriented to larger organizations, smaller entities such as local jurisdictions should review many of the same questions, scaled to their individual needs. *Every organization that owns and operates information technology equipment should have at least a rudimentary cyber security plan, and appoint an Information Security Officer (ISO) or single point of contact for cyber security, including up-to-date 24/7 contact information*. In some cases, smaller organizations may be able to obtain sample policy documents and plans from their parent organization, and tailor them. Also, smaller jurisdictions should establish cooperative agreements to obtain access to specialized assistance such as forensic analysis when required.

The online[1] version of the SEL includes not only the individual items, but links to reference material and related commercial products. Some of the software "products" useful in the cyber security area are "freeware," i.e., they are available at no cost if certain restrictions are followed. Selected freeware products are identified on the Responder Knowledge Base and linked to appropriate SEL items. Readers are also urged to review the information at the following sites, which provide valuable advice, best practices, and opportunities for support and information sharing:

**CERT® Program Virtual Training Environment (VTE)**
http://vte.cert.org
The Virtual Training Environment (VTE) is a Web-based knowledge library for information assurance, computer forensics and incident response, and other IT-related topics. VTE is produced by the CERT® program of the Software Engineering Institute at Carnegie Mellon University. While VTE is used to offer security training, DoD 8570.1 and FISMA training, and CERT® courses to partner organizations and students in an online format, CERT® makes as much of its library as possible available to the public in an effort to create a more knowledgeable information security community.

**National Institute of Standards and Technology (NIST)**
http://csrc.nist.gov/
Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. The NIST Information Technology Laboratory, Computer Security Division provides a variety of tips, newsletters, and publications to support cyber security efforts.

**US Computer Emergency Readiness Team (US CERT)**
http://www.us-cert.gov/
Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

**Multi-State Information Sharing and Analysis Center (MS-ISAC)**
http://www.cscic.state.ny.us/msisac/index.html
A public site identifying what the MS-ISAC is and what its mission, goals and objectives are in improving the nation's cyber security posture from a state and local perspective. The goal is to have this MS-ISAC include all fifty states, which would provide a valuable centrally-coordinated mechanism for sharing important security intelligence and information between the States. The MS-ISAC can serve as a critical point of contact between the States and the Federal government. A primary goal of the MS-ISAC is to eliminate duplicative efforts.

**The SANS™ Institute**
http://www.sans.org/rr (reading room) and http://isc.sans.org (Internet Storm Center)
SANS is an example of non-government cyber security resources, and is one of the largest sources for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and operates the Internet's early warning system - the Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face.

**National Security Agency Central Security Service**
http://www.nsa.gov/snac
NSA initiatives in enhancing software security cover both proprietary and open source software, and

[1] *The on-line version is available on the Responder Knowledge Base, www.rkb.mipt.org.*

they have successfully used both proprietary and open source models in their research activities. NSA's work to enhance the security of software is motivated by one simple consideration: use their resources as efficiently as possible to give NSA's customers the best possible security options in the most widely employed products. The objective of the NSA research program is to develop technologic advances that can be shared with the software development community through a variety of transfer mechanisms. NSA does not favor or promote any specific software product or business model. Rather, NSA is promoting enhanced security.

## Online Selection Factors

Like most sections in the 2006 SEL, the online version of the cyber security section uses a pair of selection factors to assist users in quickly identifying appropriate equipment items. For this section, the SubGroup chose User Level and Use Location (described below) as the two factors. Every online item is "tagged" for each appropriate combination of factors. Thus users on the online version can choose any combination of User Level and Use Location, and the system will provide a list of all items tagged for that combination.

**The User Levels for Cyber security equipment are defined as follows:**

| | |
|---|---|
| End User | Users who possess no special training or other qualifications with respect to the equipment being utilized. Examples would be personal computer users who are familiar with basic applications but have not received any classroom or advanced training. |
| IT Technician | Users who possess some specialized training or other qualifications with respect to the equipment being utilized. Examples would be users who have attended classroom training for a Geographic Information System, or who have received training in hardware installation and setup. |
| IT Advanced Technician | Users who possess some extensive training or career-level qualifications with respect to the equipment being utilized. Examples would be trained professional network administrators who possess professional qualifications such as Microsoft Certified Systems Engineer (MCSE), or computer repair professionals. |

**The probable Use Location(s) are defined as follows:**

| | |
|---|---|
| Rear Information Zone - Strategic | Emergency Operations Center/ Joint Operations Center Intel Support. |
| Rear Information Zone - Operational | Emergency Operations Center/ Departmental Operations Center Intel Support. |
| Forward Information Zone - Support [Cold] | Incident Command Post Intel Support; near incident scene, but in cold zone. |
| Forward Information Zone - Contamination Reduction [Warm] | Operations/Intel Support in warm zone. |
| Forward Information Zone - Exclusion [Hot] | Operations/Intel Support in hot zone. |

The two factors provide a method for classifying equipment items. For example, a network firewall might be classified as requiring an IT Advanced Technician to install and configure, and might be used in the Rear Information Zone or even the Forward Information Zone - Support [Cold], but would not be used in either the Warm or Hot zones. In the online SEL, if a user selected "IT Advanced Techni-

cian" and "Rear Information Zone" as the two desired selection factor values, the network firewall would then appear in the search results along with any other equipment recommended for that combination.

| Item Number/Title | Description | Features/Operating Considerations | Standards[1] |
|---|---|---|---|
| **AU - Authentication Devices** 00 | | | |
| 05AU-00-BIOM<br><br>Device, Biometric User Authentication | Devices that utilize biometric characteristics (fingerprints, palm prints, retinal scanning, etc.) to authorize access to facilities and/or systems. | May be implemented as a peripheral device or integrated into other hardware.<br>---<br>Check both "false positive" and "false negative" error rates. False positives are more serious since they validate an unauthorized user.<br>May create conflicts with other software or some operating systems - be sure to test on actual hardware/software configuration before procurement.<br>Should be used as part of a "two-factor" authentication scheme requiring an additional factor such as a password.<br>NIST Special Publication 800-76 (available in draft) provides guidance. | |
| 05AU-00-TOKN<br><br>System, Remote Authentication | System used to provide enhanced remote authentication, usually consisting of a server, some synchronization scheme, and a device, or token. | May be connected via USB or PCMCIA to remote computer.<br>Some may not be connected, but simply generate a time-based, synchronized password.<br>Provides secure (encrypted) communication to network.<br>---<br>Battery life is critical for tokens not connected to a machine.<br>Carefully check compatibility with hardware/operating system/software suite to be used.<br>May not be compatible with some applications, so that a different scheme might be necessary for initial login versus access to online application.<br>Will require management of the synchronization process, and a process for immediate cancellation of lost/stolen devices. | |
| **EN - Encryption** 00 | | | |
| 05EN-00-ECRP<br><br>Software, Encryption | Encryption software for protecting stored data files or email messages. | May integrate as "plug-in" to popular email software such as Outlook or Eudora.<br>May utilize public key cryptography, requiring the establishment of public and private keys for users.<br>---<br>See NIST Advanced Encryption Standard (AES) for applicable standards. Note that the Data Encryption Standard (which includes DES and 3-DES) is being → | 65, 88, 129 |

[1] *Use numbers given to refer to Standards List at the end of this document.*

| Item Number/Title | Description | Features/Operating Considerations | Standards[1] |
|---|---|---|---|
| **EN - Encryption**<br>00 - *Continued* | | | |
| | | replaced by AES.<br>See NIST SP 800-36 for guidance.<br>Third-party professional security audit of network recommended.<br>Planning for key management is essential, and should include a key escrow plan if critical data is being stored in encrypted format. | |
| 05EN-00-ETRN<br><br>Encryption, Data Transmission | A class of network access solutions, usually for remote access, that provide encrypted user access. May be used for remote access, point to point, or link encryption. Includes Virtual Private Networks, and encrypted transmission modes such as SSH and SSL. | Some solutions will utilize hardware "tokens" in addition to software clients (see 05AU-00-TOKN).<br>Link encryption will required devices at each end of the link.<br>Centralized management tools may be available for hardware based solutions such as link encryptors.<br>----------<br>See NIST SP 800-36 for guidance.<br>Third-party professional security audit of network recommended.<br>When utilized on handheld devices, the additional overhead may severely impact data transmission - consider platform(s).<br>Planning for key management is critical. | 65, 88, 129 |
| **HS - Host Level Security**<br>00 | | | |
| 05HS-00-MALW<br><br>Software, Malware Protection | Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments. | Workstation software should allow both scheduled and "on access" scanning.<br>----------<br>Must maintain current signature file to operate effectively - usually requires a subscription.<br>Should be deployed at the workstation, server, and firewall level for entire network segments.<br>Third-party professional security audit of network recommended to identify proper deployment and verify the effectiveness of the deployment against known threats.<br>Maintenance of current software versions for operating systems and software throughout the system is critical (including peripheral devices, network devices such as routers, and → | 129, 133, 137 |

[1] *Use numbers given to refer to Standards List at the end of this document.*

| Item Number/Title | Description | Features/Operating Considerations | Standards[1] |
|---|---|---|---|
| **HS - Host Level Security**<br>00 - *Continued* | | | |
| | | devices that only access the system periodically). | |
| 05HS-00-FRNS<br><br>Software, Forensic | Application suites that allow in-depth analysis of hosts based on operating system and file systems. Software of this type may be used by law enforcement officers, government/corporate investigators and consultants to investigate the aftermath of computer-related crimes. Forensics software generally includes disk analysis tools, tools for the recovery of deleted files, and integrated database support to mark files and data of interest to investigators. | Will support a specific list of operating systems (e.g., Windows, Linux, Solaris).<br>Will support a specific list of file systems, such as FAT12, FAT16, FAT32, NTFS, EXT2/3 (Linux), Reiser (Linux), UFS (Sun Solaris), AIX Journaling File System (JFS and jfs) LVM8. FFS (OpenBSD, NetBSD, and FreeBSD), Palm, HFS, HFS+ (Macintosh), CDFS, ISO 9660, UDF, DVD.<br>Support for evidence collection and chain of custody.<br>Analysis of Email, Internet communications, and document files.<br>----------<br>Some packages may require add-on applications.<br>Some packages may not support all file systems or OS types.<br>May require purchase of additional tools to support analysis of hand-held devices (Palm/Blackberry/etc.). | 129 |
| 05HS-00-PFWL<br><br>System, Personal Firewall | Personal firewall for operation on individual workstations. Usually a software solution, but appliances are also available. See also: 05NP-00-FWAL. | Some effective shareware available.<br>----------<br>Shareware or purchased.<br>Third-party professional security audit of network recommended.<br>May require centralized management to ensure synchronization of allowable traffic across the organization.<br>May require "baselining" against organizational policy before implementation, and → | 129, 131, 137 |

[1] *Use numbers given to refer to Standards List at the end of this document.*

| Item Number/Title | Description | Features/Operating Considerations | Standards[1] |
|---|---|---|---|
| **HS - Host Level Security**<br>00 - *Continued* | | | |
| | | should be tested to ensure that required applications work correctly when the firewall is active. | |
| **NP - Network Level Security**<br>00 | | | |
| 05NP-00-FWAL<br><br>Firewall, Network | Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL. | May implement simple filtering, or may include other functions such as malware protection (e.g., virus scanning) or application proxies.<br>---<br>See NIST SP 800-36 and SP 800-41 for guidance.<br>Third-party professional security audit of network recommended to ensure proper deployment.<br>Should reflect organization's written policy on connectivity and permitted traffic.<br>Must be capable of both inbound and outbound filtering. | 129, 131, 135, 137 |
| 05NP-00-IDS<br><br>System, Intrusion Detection | Intrusion Detection System (IDS), deployed at either host or network level to detect unauthorized or aberrant behavior on the network. Software and hardware (appliance) solutions exist. | Some IDS systems rely on signatures; others attempt to detect anomalies against baseline usage.<br>---<br>Requires trained network security personnel to configure system and interpret warning messages. Prone to false positives.<br>See NIST SP 800-36 for guidance.<br>Professional third party security audit recommended before deployment. Use of IDS systems is usually appropriate only after more basic defenses such as firewalls have been deployed. | 128, 129, 132, 134, 137 |
| 05NP-00-SCAN<br><br>Tools, Network Vulnerability Scanning | Port scanners and other tools designed to identify security vulnerabilities on networks or individual hosts on target networks. | ---<br>Best use of these tools is recurring scans against established vulnerability baseline.<br>Use with caution - some tools can bring down target hosts. Suggest scanning a small representative subset of the target network first to ensure that the scan is benign. Then scan entire network. → | 129, 137 |

[1] *Use numbers given to refer to Standards List at the end of this document.*

| Item Number/Title | Description | Features/Operating Considerations | Standards[1] |
|---|---|---|---|
| **NP - Network Level Security**<br>00 - *Continued* | | | |
| | | These tools do not simulate an attack. They merely identify known vulnerabilities. The best way to establish a "real" vulnerability baseline is through a third-party vulnerability assessment. | |
| 05NP-00-SEIM<br><br>System, Security Event/Incident Management | Software or appliance that gathers data from multiple security sources such as firewalls, intrusion detection systems, malware protection systems, etc. to provide log file consolidation and event correlation capability in support of network security operations. | Provides agents to interface with existing security applications and devices.<br>Offers centralized management and storage of data from agents.<br>May provide visualization tools such as a graphic representation of enterprise security statistics.<br>---<br>Check whether agents are available for all currently-fielded software and devices.<br>Obtain complete pricing for baseline package, all required agents, and add-on software such as report generators before procurement.<br>Implementation of this type of product creates a significant attack target for intruders. Care must be taken to secure the management system against attack. | 129 |
| **PM - Patch and Configuration Management**<br>00 | | | |
| 05PM-00-PTCH<br><br>System, Patch/Configuration Management | System to manage the update and installation of patches, applications, and/or operating systems, utilized by an organization in order to maintain current "version control." | Record keeping of existing versions on different clients, date of last change, etc.<br>System automatically gathers current versions from assorted vendors for pushing out to clients.<br>---<br>May require the installation of client software on all managed devices (workstations, servers, etc.). This can be a significant task, and any required client software should be checked for compatibility with hardware/operating system/software suites in use prior to procurement.<br>Some products may track only operating system software. However, vulnerabilities in applications and network devices such as routers are also important and should be included in any patch management plan.<br>Regular third-party vulnerability assessments should also be performed. | 130 |

[1] *Use numbers given to refer to Standards List at the end of this document.*